NMCI

NAVY MARINE CORPS INTRANET

Public Key Infrastructure

Using Your Common Access Card with NMCI

An Introduction

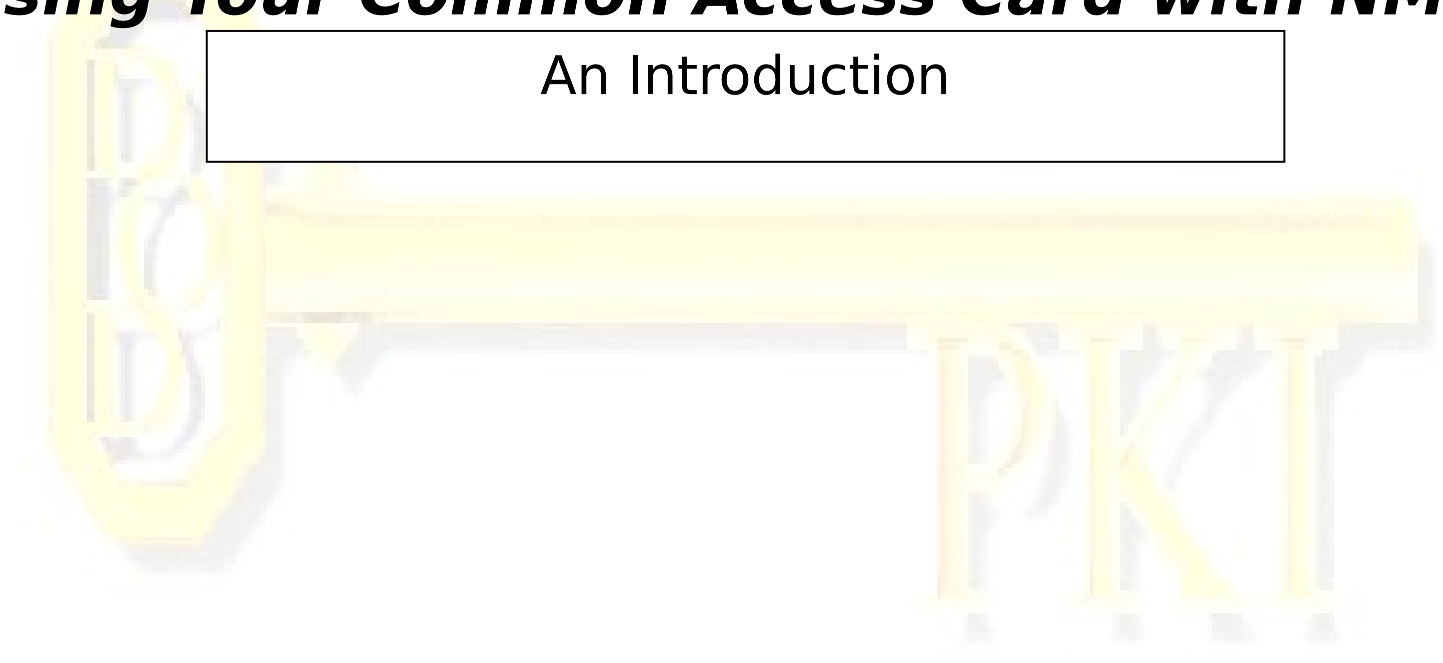


Table of Contents

Module contents include:

I. PKI Policy

II. Elements of PKI

III. Preparing for PKI: User Responsibilities

IV. Introduction to Digital Signatures

V. Configuring Your NMCI Seat for PKI

VI. Digitally Signing and Encrypting Email

VII. Opening Digitally Signed Email

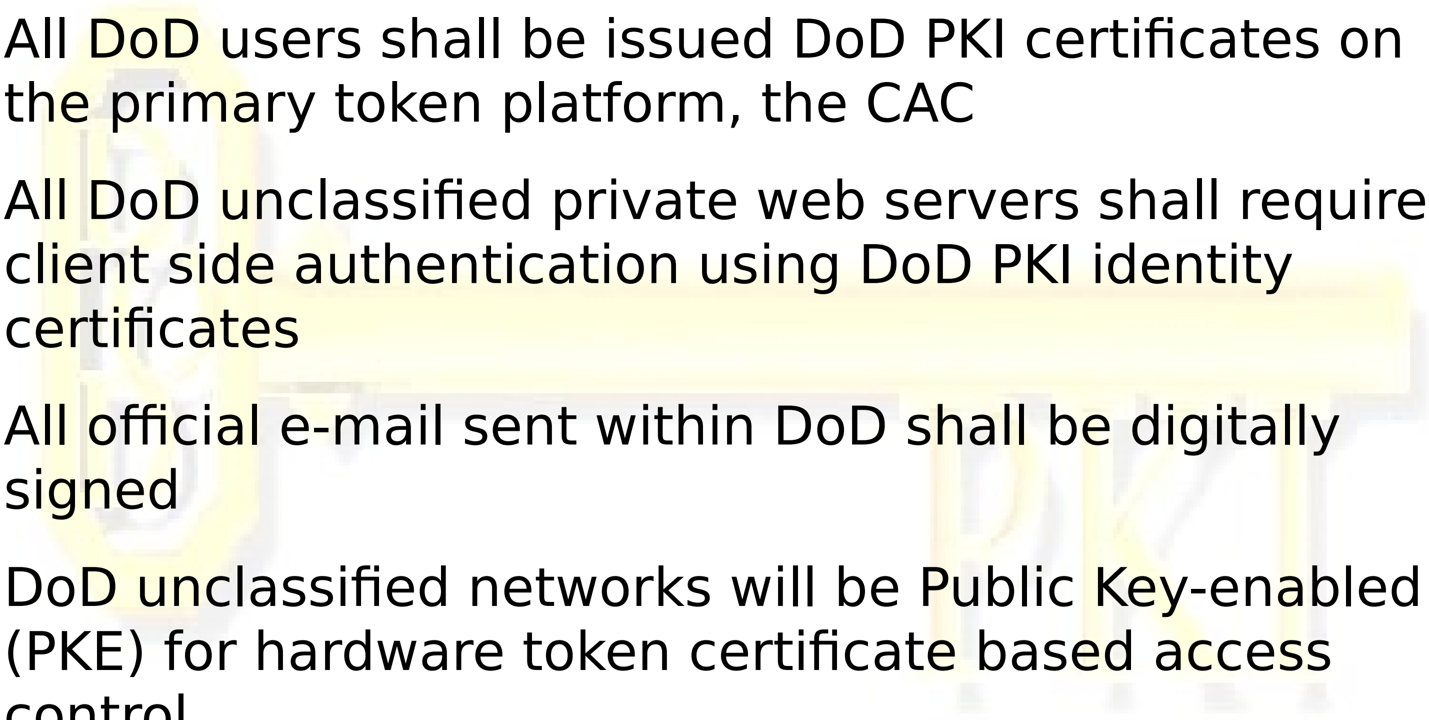
VIII. Authenticating to Public Key-enabled Websites

IX. Accessing Websites that Issue Digital Certificates

X. CAC Maintenance

DoD Policy on PKI

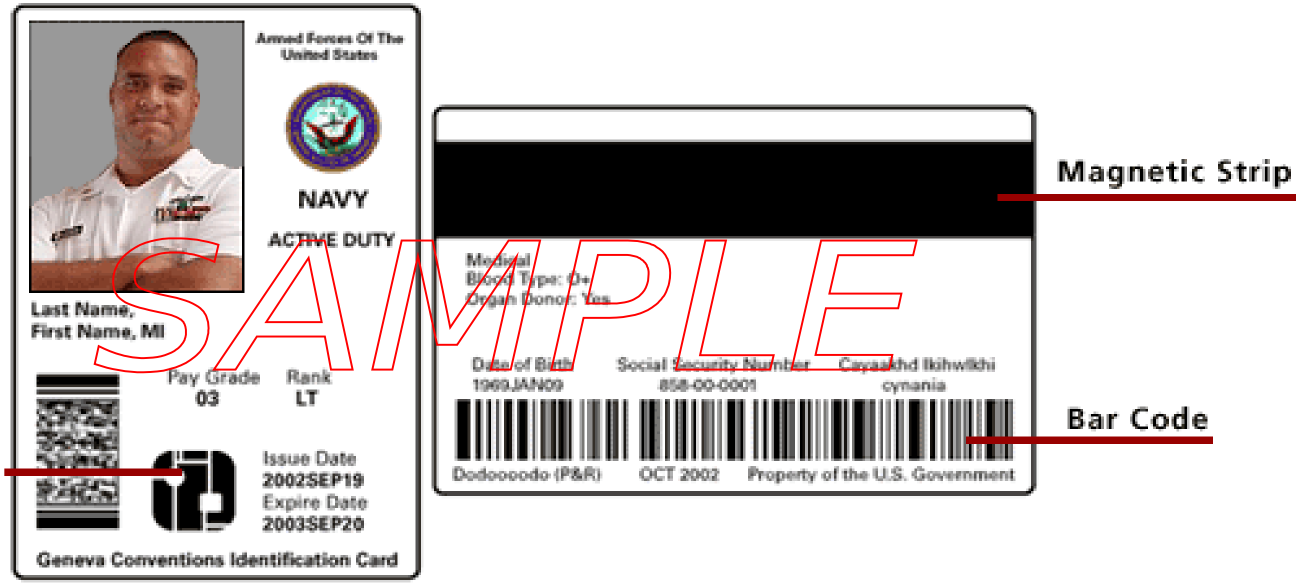
By October 2004:



- ✓ All DoD users shall be issued DoD PKI certificates on the primary token platform, the CAC
- ✓ All DoD unclassified private web servers shall require client side authentication using DoD PKI identity certificates
- ✓ All official e-mail sent within DoD shall be digitally signed
- ✓ DoD unclassified networks will be Public Key-enabled (PKE) for hardware token certificate based access control

The Common Access Card (CAC)

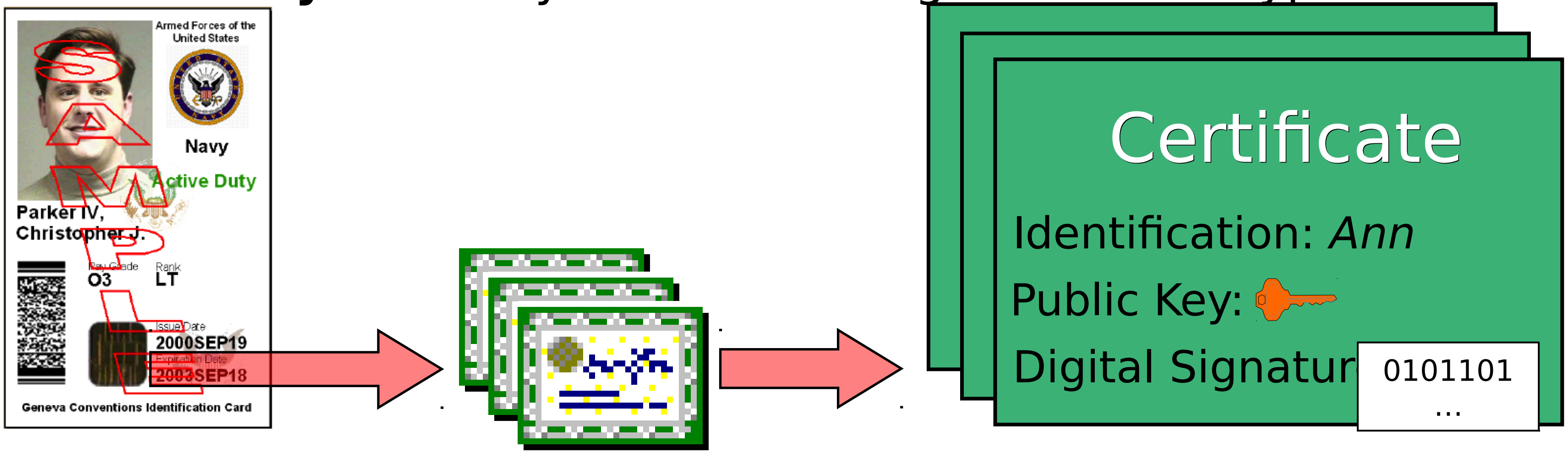
- **Small programmable, processing capable, storage devices**
- **Advantages**
  - Can store user information in multiple forms
  - Can be reprogrammed with new information



INTEGRATED CIRCUIT CHIP
contains identity, signature, and email encryption digital certificates

Elements of PKI

- **CAC –** Primary storage device for private keys and certificates
    - Contents:
        - Private Data Area (Name, SSN, DoB, Pay Grade, etc.)
        - 3 Certificates (Identity, Email Digital Signature, Email Encryption Key)
- **Digital Certificate –** Software (i.e., floppy disk) or hardware token (i.e., CAC) file containing user’s identity data and public key
    - Certificates bind identity to the private key
- **Private Key –** Privately held string used to decrypt data
- **Public Key** – Publicly available string used to encrypt data


Armed Forces of the United States
Navy
Active Duty
Parker IV, Christopher J.
Pay Grade
O3
Rank
LT
Issue Date
2000SEP19
Expiration Date
2003SEP18
Geneva Conventions Identification Card
SAMPLE

Certificate

Identification: *Ann*

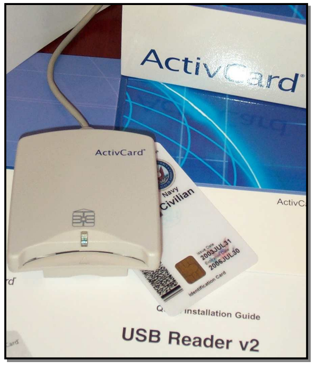
Public Key:

Digital Signatur

0101101
…

Elements of PKI *(cont)*

- **Card Reader** – Computer’s hardware interface for the CAC; integrated with keyboard for desktops, card slot found on the side of portables



- **Middleware** – Current version, ActiveCard Gold 2.2, has a utility through which users can view their CAC certificates
- **Certificate Validation Software** – Verifies certificates are trusted, not expired, and not revoked
- **Certificate Authority and Certificate Validation Infrastructure** – EDS responsible for implementation (TBD)

NMCI
NAVY MARINE CORPS INTRANET

Preparing for PKI

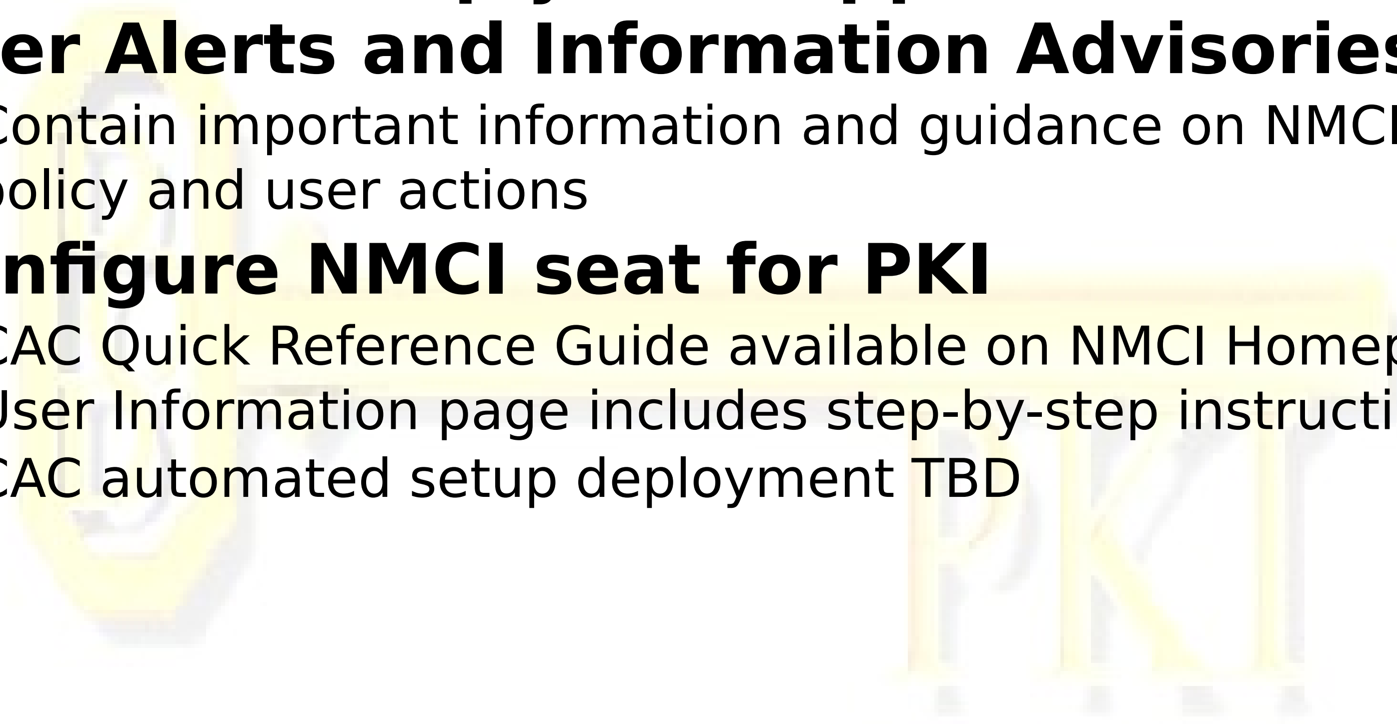
An NMCI User's Responsibilities

Preparing for PKI
User Responsibilities

- **Update CAC at local RAPIDS workstation**
  - CACs with certificates issued prior to 19 May 2002 must be updated to enable CAC-based (cryptographic) logon to NMCI
  - NMCI email account address on CAC -- interoperability requirement
  - DoD RAPIDS Site Locator at http://www.dmdc.osd.mil/rsl
- **Complete eLearning on NMCI *Homeport***
  - Search catalog for “CAC” or “PKI” at http://training/
  - Counted towards a user’s annual Information Assurance training requirement
- **Remember Personal Identification Number (PIN)**
  - Protects the user’s private information on the CAC
  - User assigns during CAC issuance
  - Prompted at NMCI login screen
  - CAC locks if PIN entered incorrectly 3 times→ requires visit to RAPIDS

Preparing for PKI
User Responsibilities (cont)

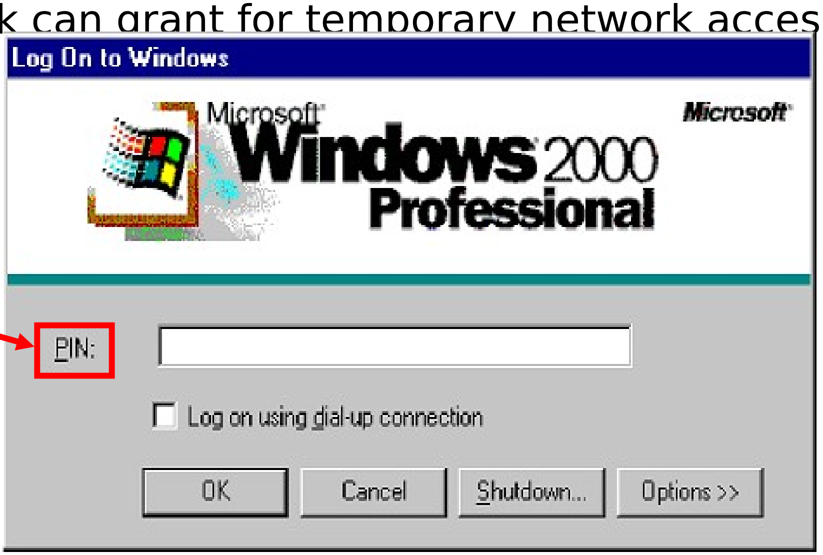
- **Read and comply with applicable NMCI User Alerts and Information Advisories**
  - Contain important information and guidance on NMCI policy and user actions
- **Configure NMCI seat for PKI**
  - CAC Quick Reference Guide available on NMCI Homeport User Information page includes step-by-step instructions
  - CAC automated setup deployment TBD



Preparing for PKI
User Responsibilities (cont)

- **Employ CAC-based cryptographic logon to access network**
  - Users will be forced to discontinue username/password network authentication and must use the CAC to access NMCI
  - NMCI Help Desk can grant for temporary network access for users who forget PIN/CAC

User-assigned PIN required for network access



CAC-based NMCI Logon Window

- **Sign and encrypt email**
  - Capability supported by Outlook on NMCI today
  - CAC must contain digital signature and email encryption certificate
  - Encryption requires possession of destination user’s public key (GAL availability TBD)

NMCI
NAVY MARINE CORPS INTRANET

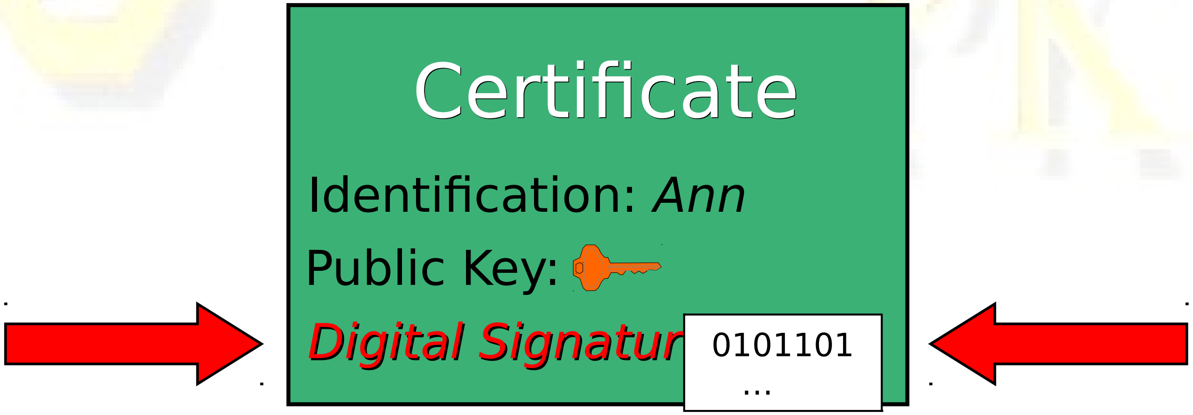
Introduction to Digital Signatures

Digital Signatures

- **Signatures are used to confirm authenticity**
  - Contracts, agreements, commitments, documents
- **A digital signature is a unique electronic value that produces the same effect as a real signature**
- **The Federal Electronic Signatures Act makes electronic signatures a legal form of authentication**
  - The act, referred to as the *e-Signature Law*, took effect Oct. 1, 2000

Digital Signatures *(cont)*

- **Must meet two primary conditions**
  - They must not be forgeable
  - They must be authentic
- **Additional desirable conditions**
  - Not alterable
  - Not reusable
- **Digital signatures provide *Non-repudiation***
  - Non-repudiation is the elimination of an individual’s ability to deny that they have participated in a transaction
  - Also ensures data integrity of message



Certificate

Identification: *Ann*

Public Key:

Digital Signatur

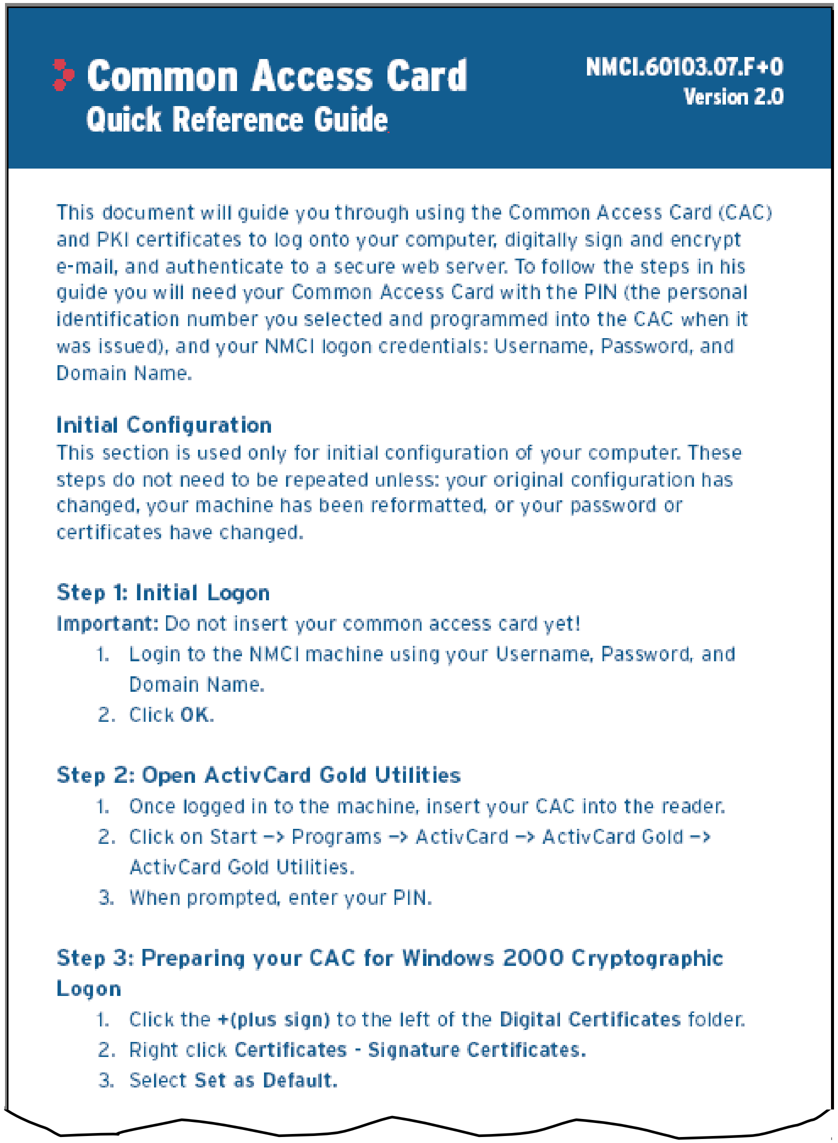
NMCI

NAVY MARINE CORPS INTRANET

Configuring Your NMCI Seat for PKI

Configuring Your NMCI Seat for PKI

NMCI
NAVY MARINE CORPS INTRANET



Common Access Card
Quick Reference Guide

NMCI.60103.07.F+0
Version 2.0

This document will guide you through using the Common Access Card (CAC) and PKI certificates to log onto your computer, digitally sign and encrypt e-mail, and authenticate to a secure web server. To follow the steps in his guide you will need your Common Access Card with the PIN (the personal identification number you selected and programmed into the CAC when it was issued), and your NMCI logon credentials: Username, Password, and Domain Name.

Initial Configuration
This section is used only for initial configuration of your computer. These steps do not need to be repeated unless: your original configuration has changed, your machine has been reformatted, or your password or certificates have changed.

Step 1: Initial Logon
Important: Do not insert your common access card yet!

1. Login to the NMCI machine using your Username, Password, and Domain Name.
2. Click **OK**.

Step 2: Open ActivCard Gold Utilities

1. Once logged in to the machine, insert your CAC into the reader.
2. Click on Start –> Programs –> ActivCard –> ActivCard Gold –> ActivCard Gold Utilities.
3. When prompted, enter your PIN.

Step 3: Preparing your CAC for Windows 2000 Cryptographic Logon

1. Click the **+(plus sign)** to the left of the **Digital Certificates** folder.
2. Right click **Certificates - Signature Certificates.**
3. Select **Set as Default.**

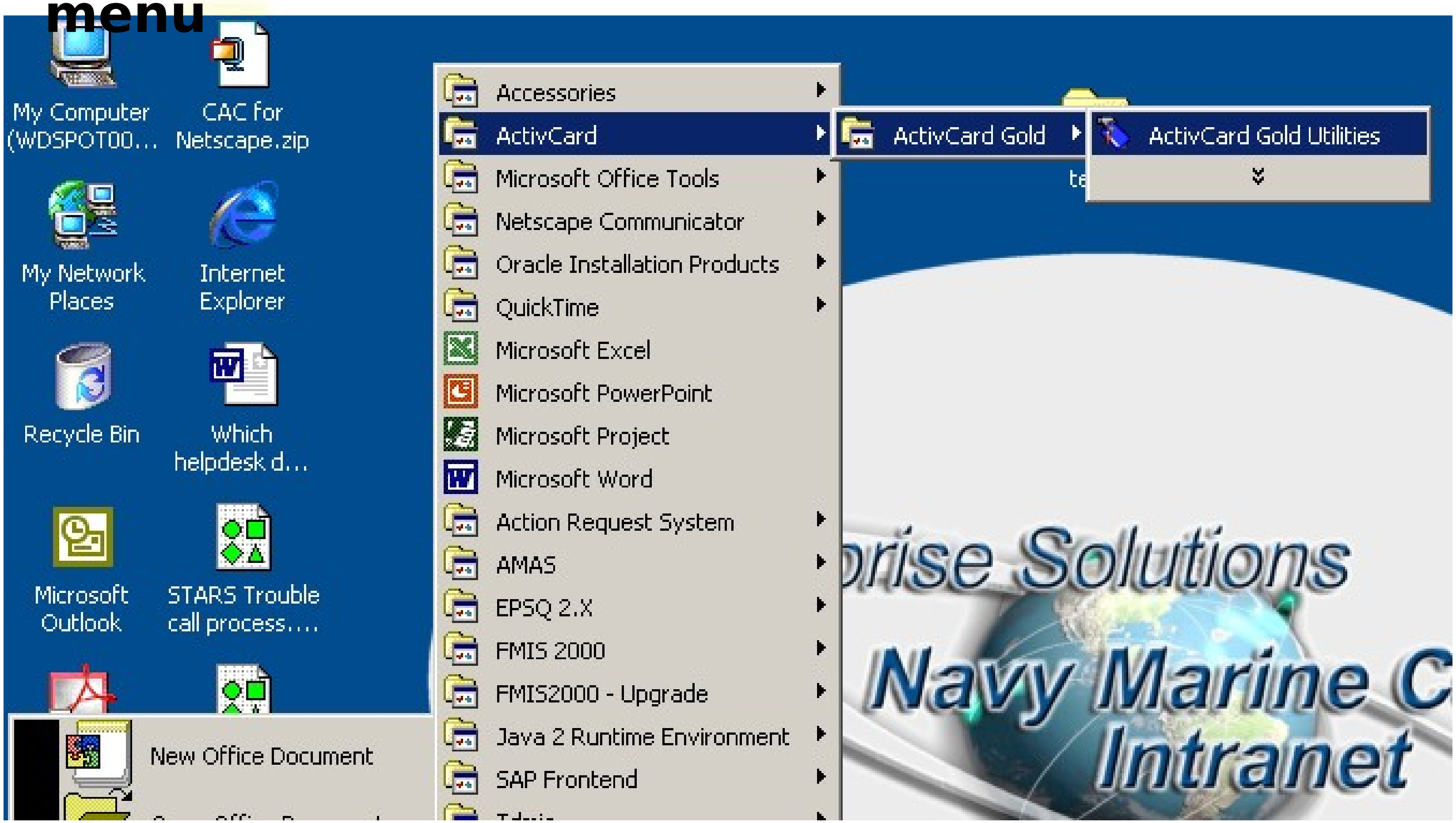
- ✓ Download CAC Quick Reference Guide at: http://training/elements/userinfo/
- ✓ Follow step-by-step procedures for registering PKI certificates and configuring Outlook

- ❖ ***Leave-behind transition (i.e.,Operational Readiness) packages provided by EDS during seat deployment should include CAC and PKI support materials***

THE FOLLOWING SLIDES DEMONSTRATE WHAT A USER WILL EXPERIENCE WHILE CONFIGURING AN NMCI SEAT FOR PKI

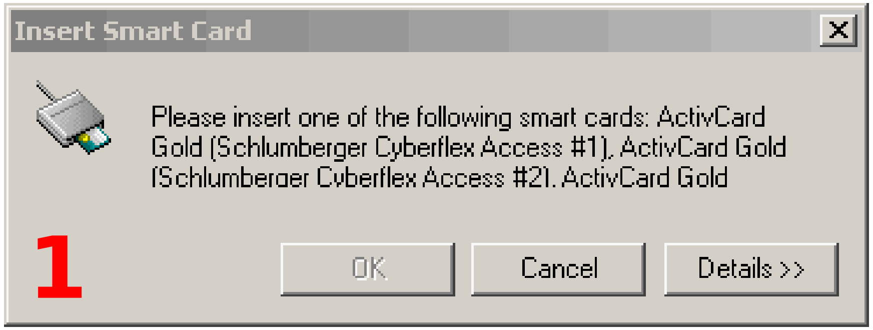
Registering Your CAC Certificates

- ✓ **Open *ActiveCard Gold* Utilities from Windows Start menu**



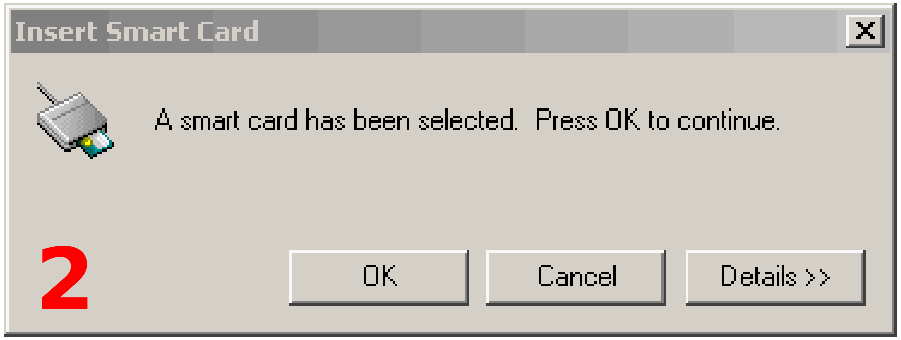
Registering Your CAC Certificates *(cont)*

- ✓ **Insert CAC and enter PIN when prompted**



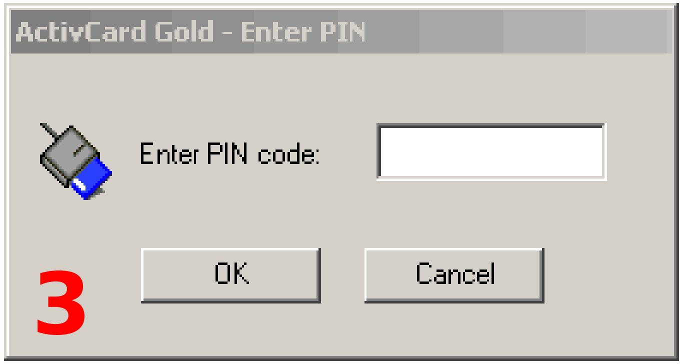
Insert Smart Card

Please insert one of the following smart cards: ActivCard Gold (Schlumberger Cyberflex Access #1), ActivCard Gold (Schlumberger Cyberflex Access #2), ActivCard Gold



Insert Smart Card

A smart card has been selected. Press OK to continue.

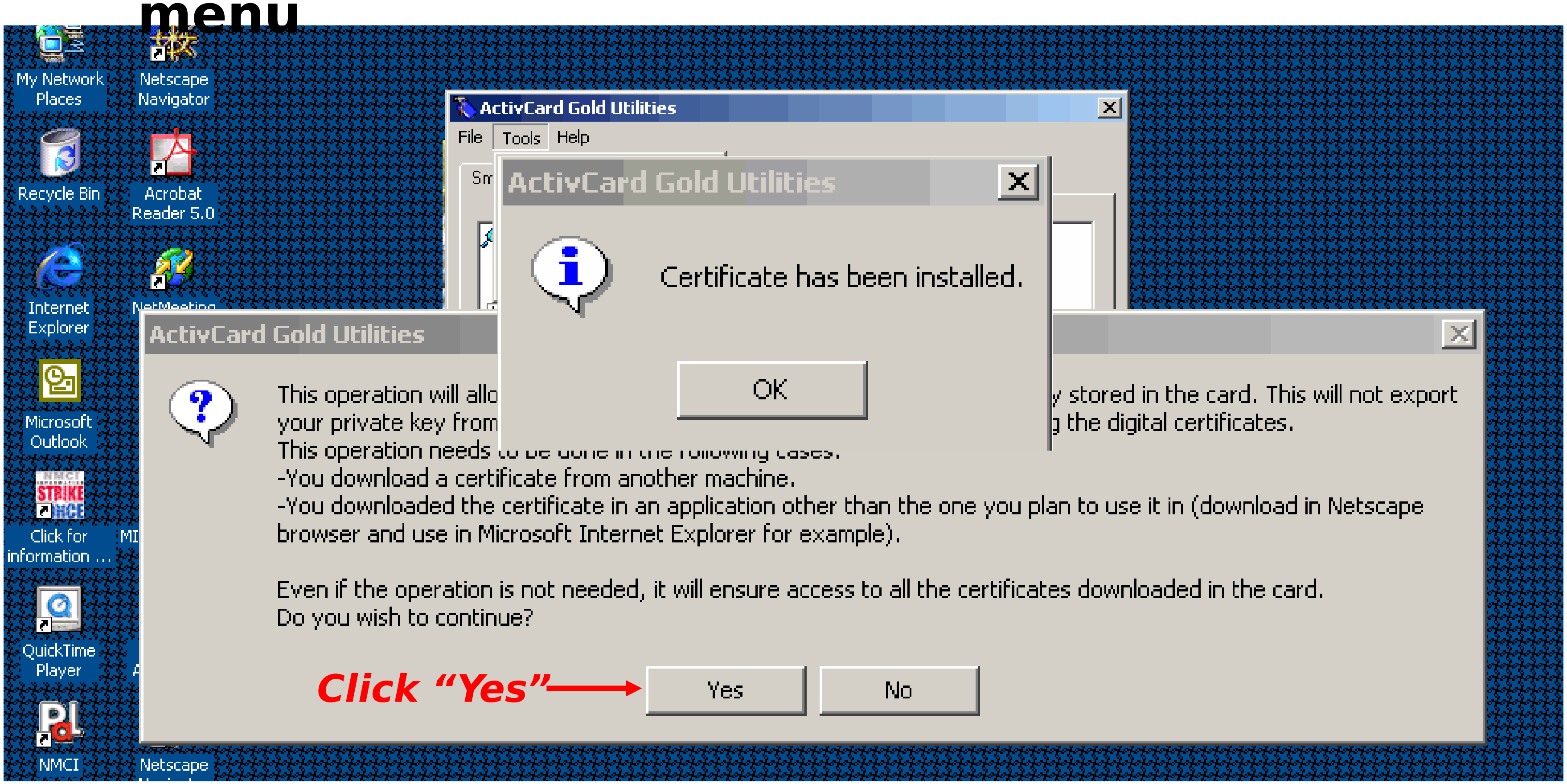


ActivCard Gold - Enter PIN

Enter PIN code:

Registering Your CAC Certificates *(cont)*

- ✓ **Select “Register Certificates” from Tools menu**



ActivCard Gold Utilities

Certificate has been installed.

ActivCard Gold Utilities

This operation will allo... y stored in the card. This will not export your private key from... g the digital certificates.
This operation needs to be done in the following cases:
-You download a certificate from another machine.
-You downloaded the certificate in an application other than the one you plan to use it in (download in Netscape browser and use in Microsoft Internet Explorer for example).

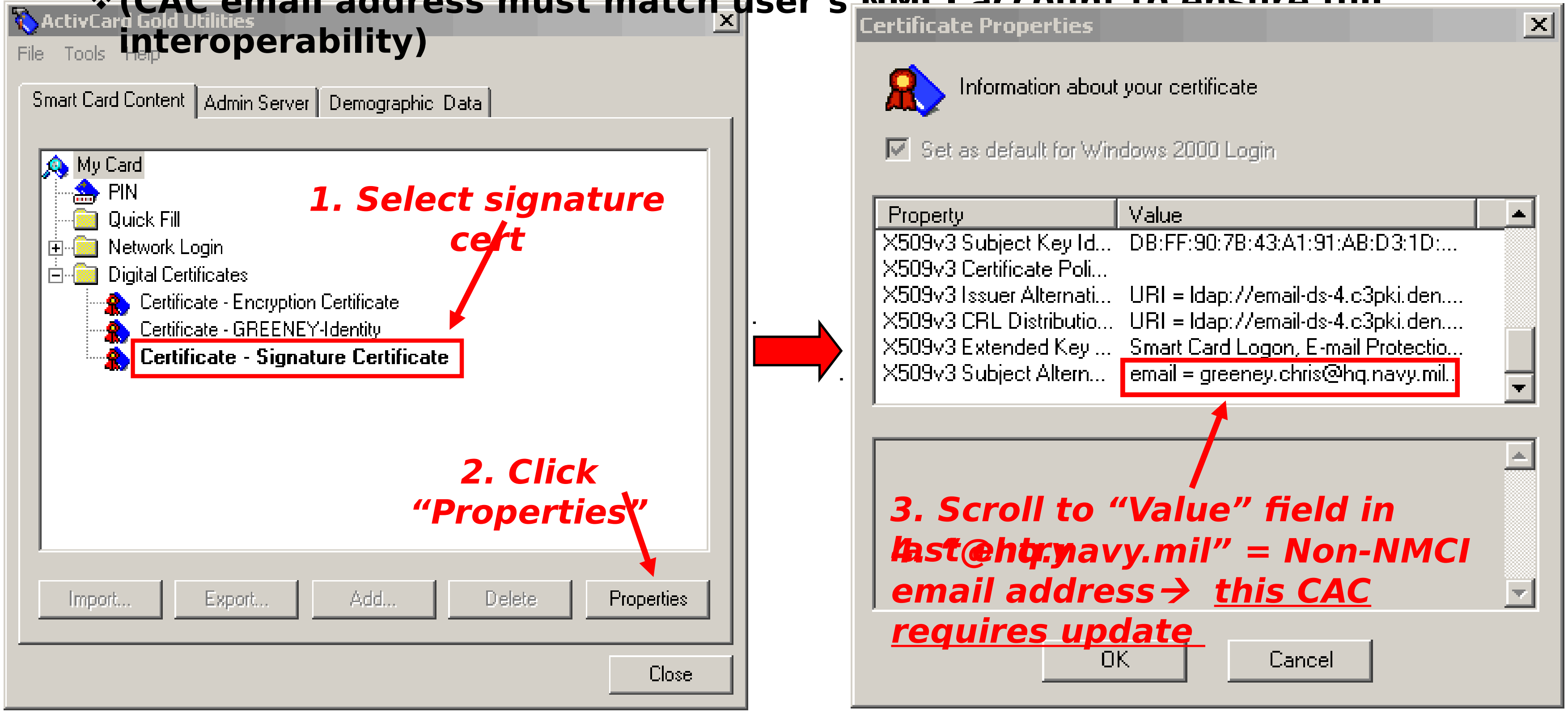
Even if the operation is not needed, it will ensure access to all the certificates downloaded in the card.
Do you wish to continue?

Click “Yes”

Viewing Your CAC Certificates

NMCI
NAVY MARINE CORPS INTRANET

- ✓ Expand Digital Certificates folder while in *ActiveCard Gold* Utilities
- ✓ If available, verify email address on CAC by viewing digital signature certificate properties (last entry)
  - ❖ (CAC email address must match user's NMCI account to ensure full interoperability)



ActivCard Gold Utilities

Certificate - Encryption Certificate
Certificate - GREENEY-Identity
Certificate - Signature Certificate

1. Select signature cert

2. Click "Properties"

Certificate Properties

Information about your certificate

☑ Set as default for Windows 2000 Login

Property	Value
X509v3 Subject Key Id...	DB:FF:90:7B:43:A1:91:AB:D3:1D:...
X509v3 Certificate Poli...	
X509v3 Issuer Alternati...	URI = ldap://email-ds-4.c3pki.den....
X509v3 CRL Distributio...	URI = ldap://email-ds-4.c3pki.den....
X509v3 Extended Key ...	Smart Card Logon, E-mail Protectio...
X509v3 Subject Altern...	email = greeney.chris@hq.navy.mil...

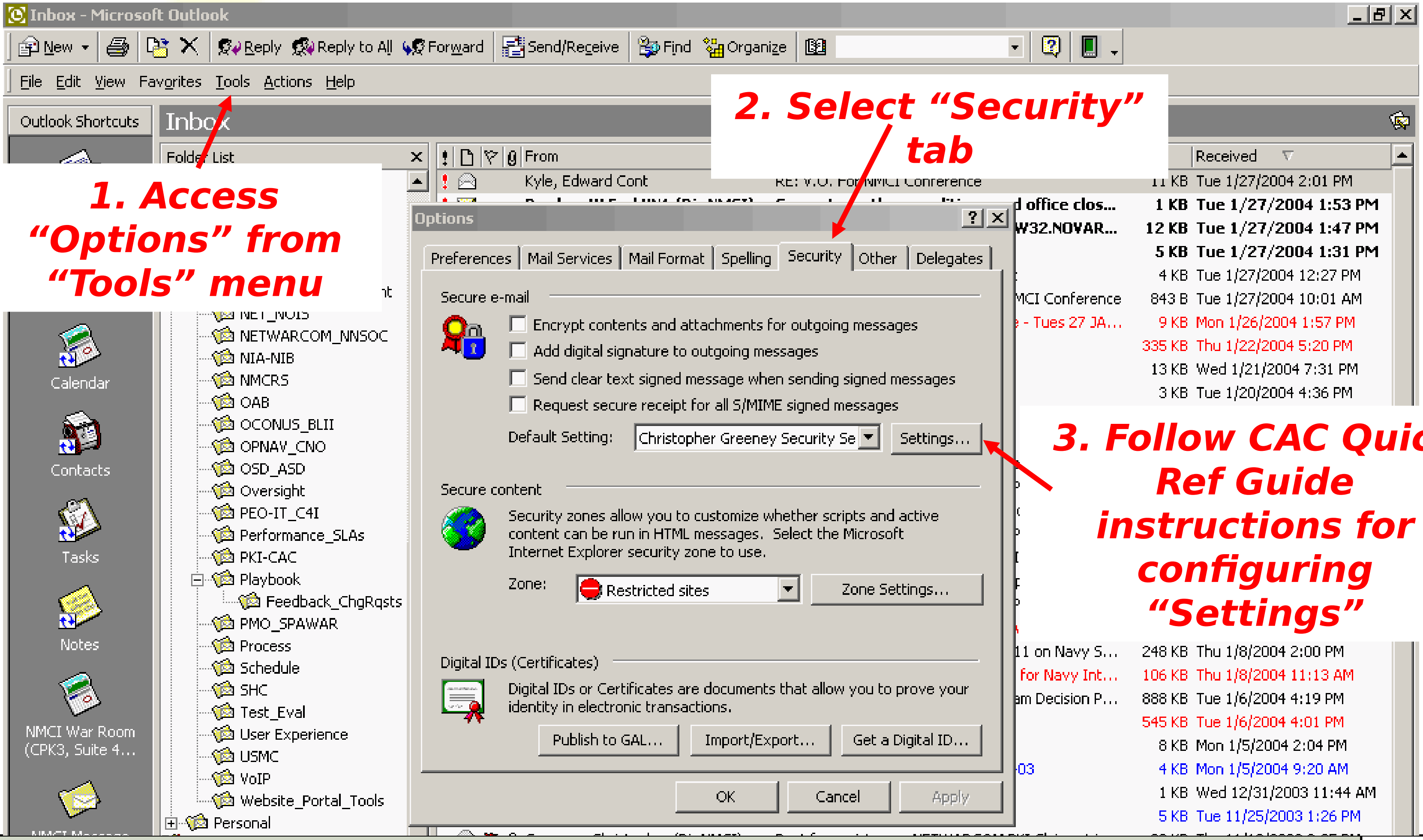
3. Scroll to "Value" field in last entry

4. "@hq.navy.mil" = Non-NMCI email address→ this CAC requires update

Configuring Microsoft Outlook

NAVY MARINE CORPS INTRANET

- ✓ **Assign email certificates to perform digital signature and message encryption functions**



Options

Preferences | Mail Services | Mail Format | Spelling | Security | Other | Delegates

Secure e-mail

- ☐ Encrypt contents and attachments for outgoing messages
- ☐ Add digital signature to outgoing messages
- ☐ Send clear text signed message when sending signed messages
- ☐ Request secure receipt for all S/MIME signed messages

Default Setting: Christopher Greeney Security Se ▾ Settings...

Secure content

Security zones allow you to customize whether scripts and active content can be run in HTML messages. Select the Microsoft Internet Explorer security zone to use.

Zone: Restricted sites ▾ Zone Settings...

Digital IDs (Certificates)

Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions.

Publish to GAL... | Import/Export... | Get a Digital ID...

OK | Cancel | Apply

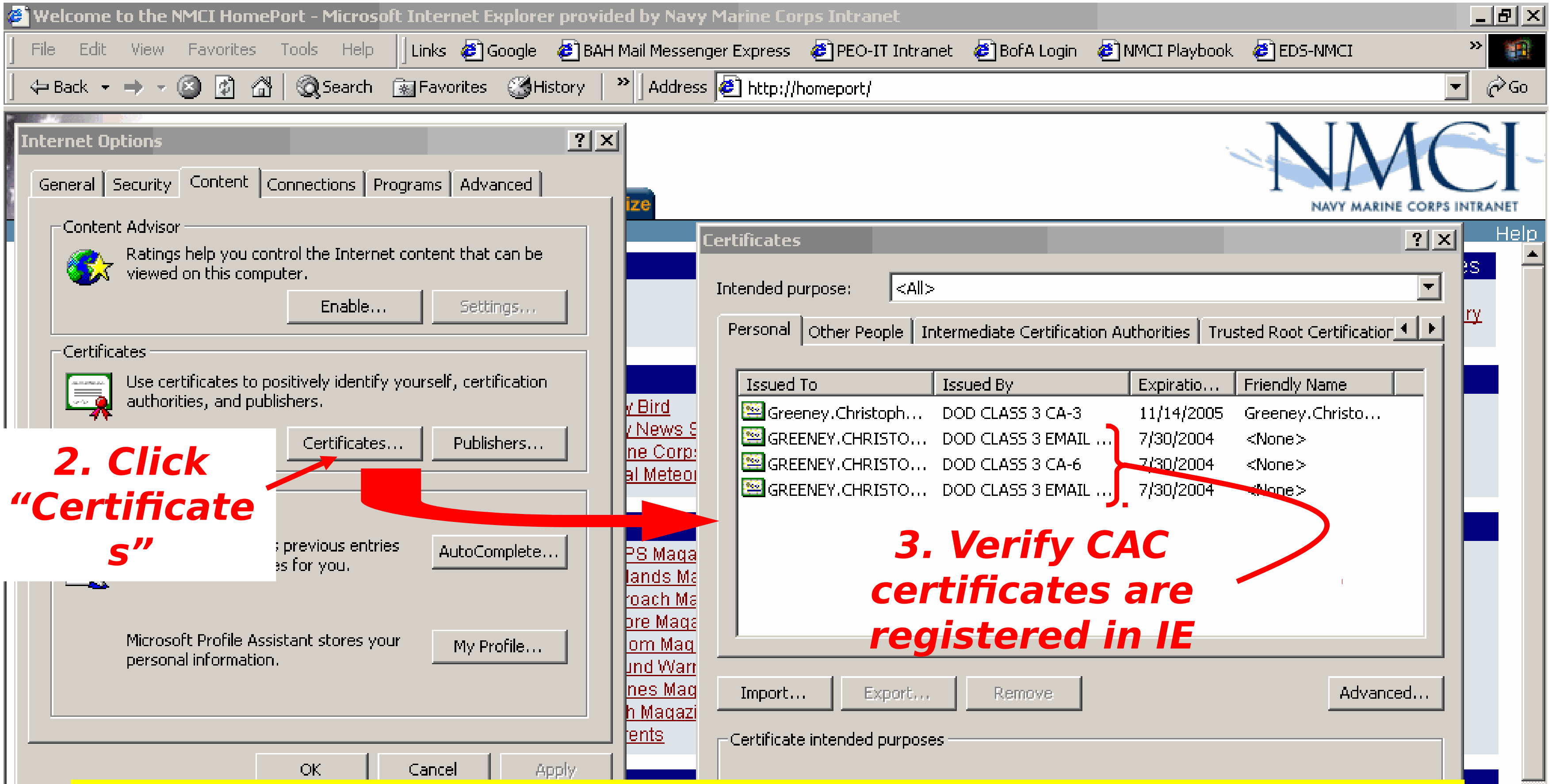
1. Access "Options" from "Tools" menu

2. Select "Security" tab

3. Follow CAC Quick Ref Guide instructions for configuring "Settings"

Verifying Internet Explorer Configuration

- ✓ ***ActiveCard Gold*** **should automatically register certificates in Microsoft Internet Explorer**



Welcome to the NMCI HomePort - Microsoft Internet Explorer provided by Navy Marine Corps Intranet
File Edit View Favorites Tools Help
Links Google BAH Mail Messenger Express PEO-IT Intranet BofA Login NMCI Playbook EDS-NMCI
Back Search Favorites History
Address http://homeport/
Go
Internet Options
General Security Content Connections Programs Advanced
Content Advisor
Ratings help you control the Internet content that can be viewed on this computer.
Enable... Settings...
Certificates
Use certificates to positively identify yourself, certification authorities, and publishers.
Certificates... Publishers...
previous entries
s for you.
AutoComplete...
Microsoft Profile Assistant stores your personal information.
My Profile...
OK Cancel Apply
NMCI
NAVY MARINE CORPS INTRANET
Help
Certificates
Intended purpose: <All>
Personal Other People Intermediate Certification Authorities Trusted Root Certification
Import... Export... Remove Advanced...
Certificate intended purposes

Issued To	Issued By	Expiratio...	Friendly Name
Greeney.Christoph...	DOD CLASS 3 CA-3	11/14/2005	Greeney.Christo...
GREENEY.CHRISTO...	DOD CLASS 3 EMAIL ...	7/30/2004	<None>
GREENEY.CHRISTO...	DOD CLASS 3 CA-6	7/30/2004	<None>
GREENEY.CHRISTO...	DOD CLASS 3 EMAIL ...	7/30/2004	<None>

2. Click “Certificates”

3. Verify CAC certificates are registered in IE

See CAC Quick Reference Guide for Netscape Navigator support

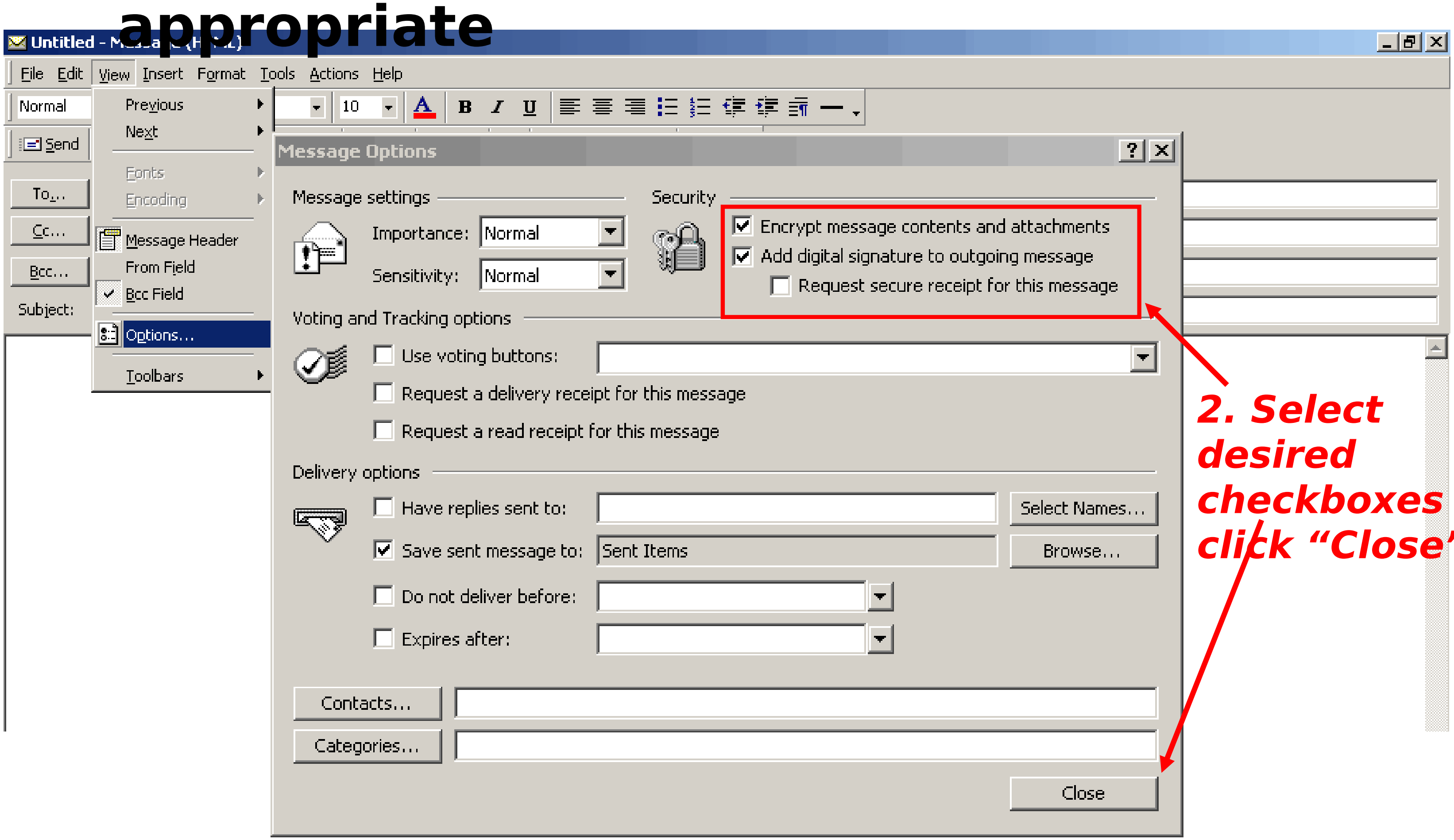
NMCI

NAVY MARINE CORPS INTRANET

Signing and Encrypting Email

Sign and Encrypt Email

✓ **Select email “Security Options” as appropriate**



Message settings

Importance: Normal

Sensitivity: Normal

Security

☑ Encrypt message contents and attachments

☑ Add digital signature to outgoing message

□ Request secure receipt for this message

Voting and Tracking options

□ Use voting buttons:

□ Request a delivery receipt for this message

□ Request a read receipt for this message

Delivery options

□ Have replies sent to: Select Names...

☑ Save sent message to: Sent Items Browse...

□ Do not deliver before:

□ Expires after:

Contacts...

Categories...

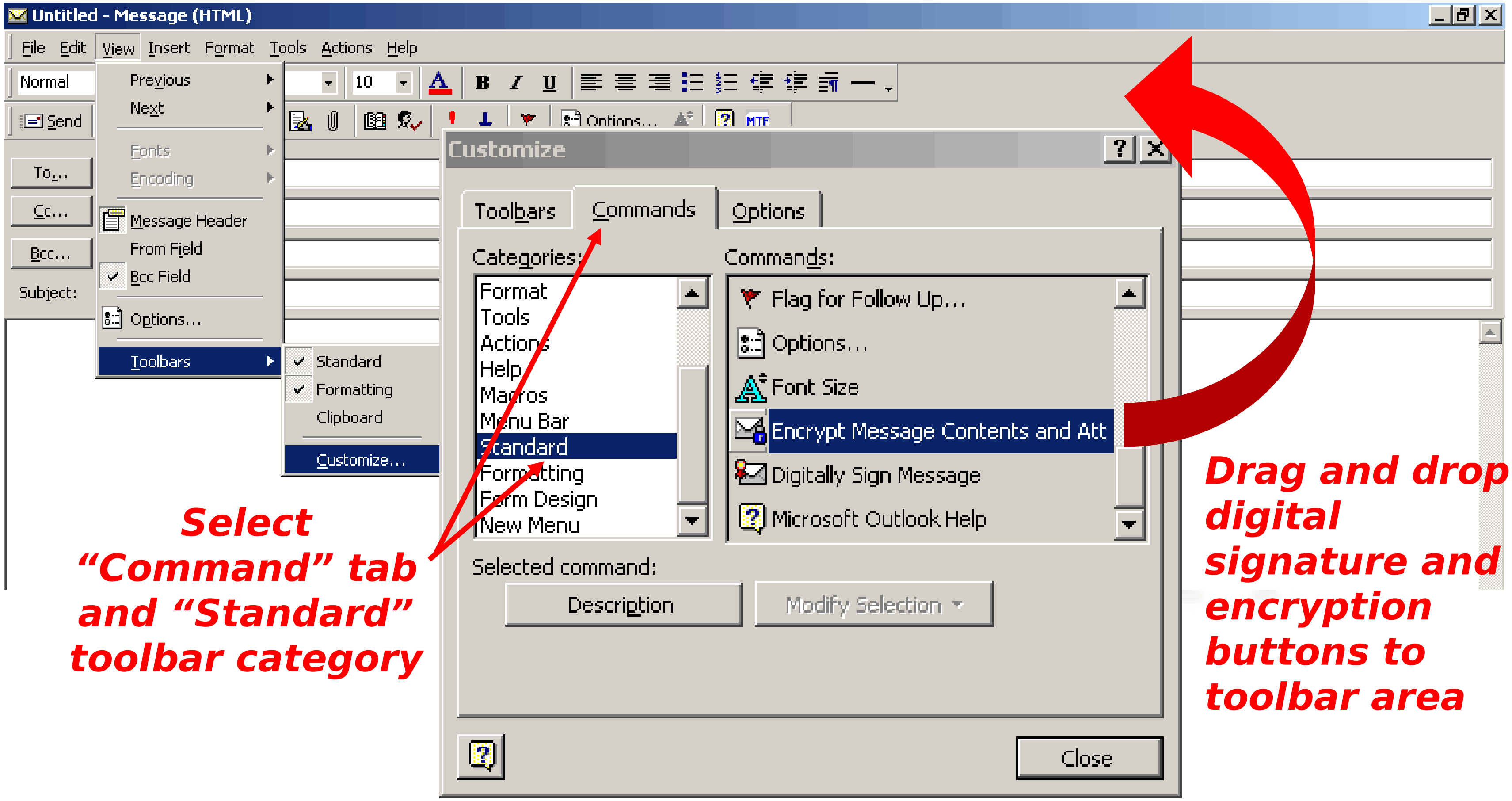
Close

2. Select desired checkboxes and click “Close”

Sign and Encrypt Email *(cont)*

NMCI NAVY MARINE CORPS INTRANET

- ✓ **Add digital signature and encryption shortcut buttons to email toolbar**

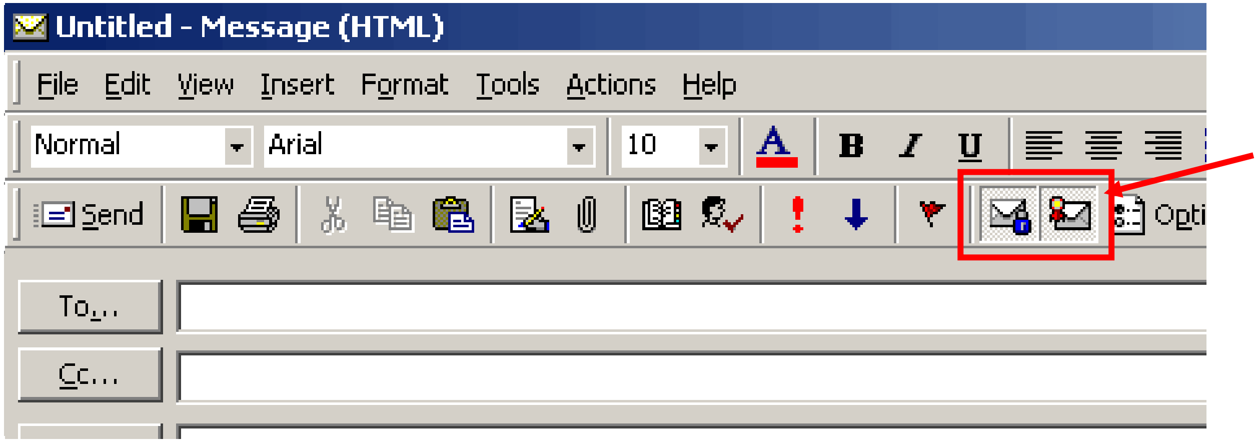


Select "Command" tab and "Standard" toolbar category

Drag and drop digital signature and encryption buttons to toolbar area

Sign and Encrypt Email

- ✓ **Digitally sign and encrypt email messages using toolbar shortcuts**


Untitled - Message (HTML)
File Edit View Insert Format Tools Actions Help
Normal
Arial
10
B I U
Send
Opti
To...
Cc...

Click appropriate buttons to encrypt message (blue lock icon) or to digitally sign (red certificate icon)

Highlighted buttons indicate message will be encrypted and/or digitally signed when sent

NMCI
NAVY MARINE CORPS INTRANET

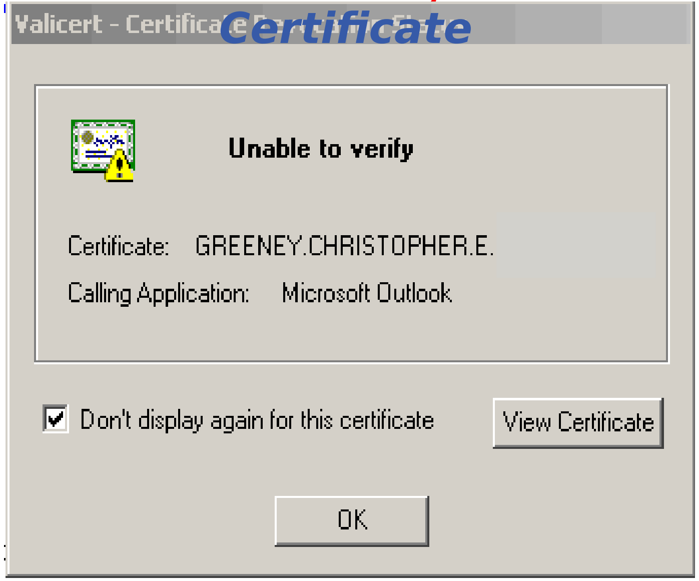
Opening Digitally Signed Email

What You Can Expect

Opening Digitally Signed Email

- **"Desktop Validator" software resides on NMCI seat and interacts with Microsoft Windows applications**
  - Outlook – digitally signed emails
  - Internet Explorer – sites issuing certificates from Web server
  - Users will experience delay in opening signed mails or accessing certificate-issuing Web sites during validation process

Unknown Certificate



Valicert - Certificate Revocation Status

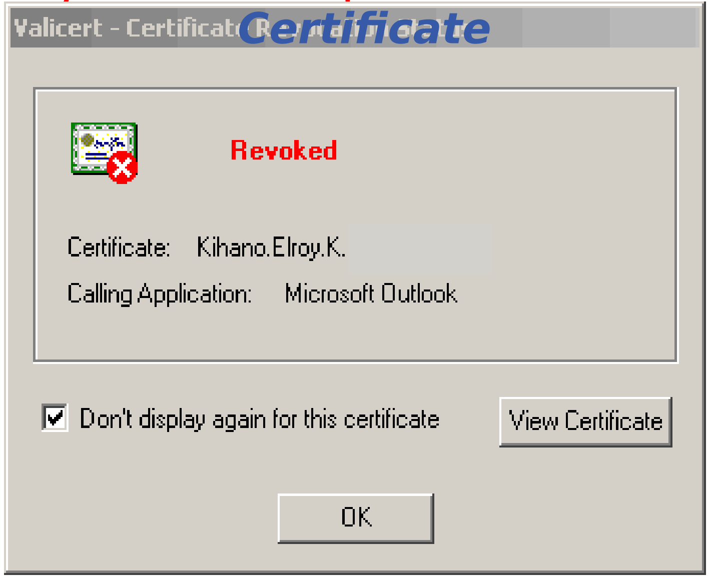
Unable to verify

Certificate: GREENEY.CHRISTOPHER.E.

Calling Application: Microsoft Outlook

☑ Don't display again for this certificate

Revoked Certificate



Valicert - Certificate Revocation Status

Revoked

Certificate: Kihano.Elroy.K.

Calling Application: Microsoft Outlook

☑ Don't display again for this certificate

Note: No alert will appear for trusted certificates

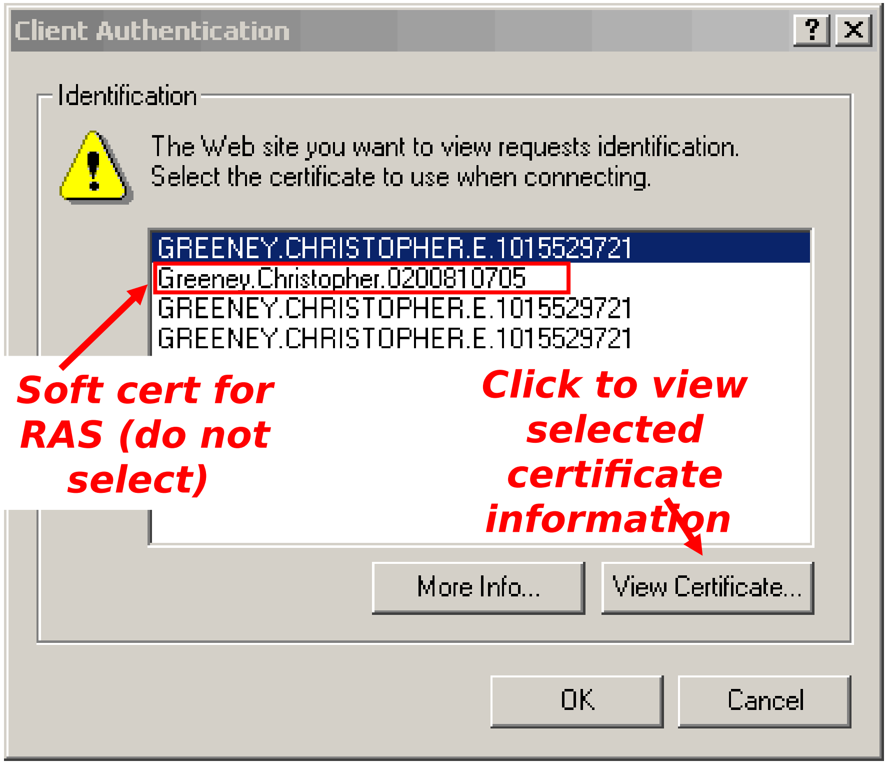
NMCI

NAVY MARINE CORPS INTRANET

Authenticating to Public Key-enabled Web Sites

Secure Web Server Authentication

- ✓ **Public Key-enabled Private DoD Web sites will automatically invoke Internet Explorer Client Authentication dialogue box**
- ✓ **Select a certificate**
  - ❖ **In most cases, CAC-based Identity cert is preferred—must “View Certificate” to verify**

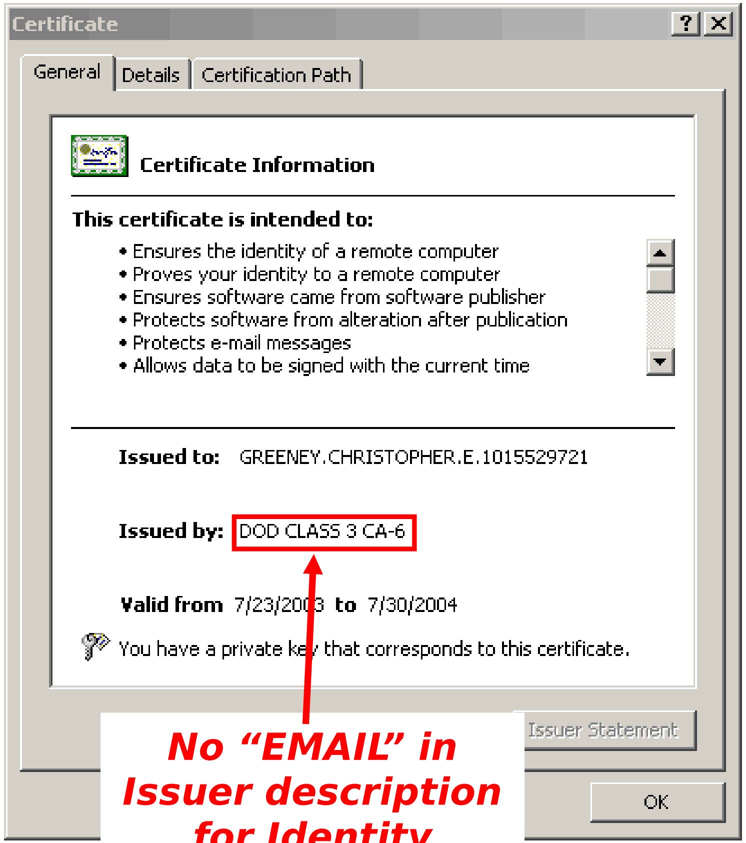


The Web site you want to view requests identification.
Select the certificate to use when connecting.

GREENEY.CHRISTOPHER.E.1015529721
Greeney.Christopher.0200810705
GREENEY.CHRISTOPHER.E.1015529721
GREENEY.CHRISTOPHER.E.1015529721

Soft cert for RAS (do not select)

Click to view selected certificate information



Certificate Information

This certificate is intended to:

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- Ensures software came from software publisher
- Protects software from alteration after publication
- Protects e-mail messages
- Allows data to be signed with the current time

Issued to: GREENEY.CHRISTOPHER.E.1015529721

Issued by: DOD CLASS 3 CA-6

Valid from 7/23/2003 **to** 7/30/2004

You have a private key that corresponds to this certificate.

No “EMAIL” in Issuer description for Identity certificate

NMCI
NAVY MARINE CORPS INTRANET

Accessing Web Sites That Issue Certificates

What You Can Expect

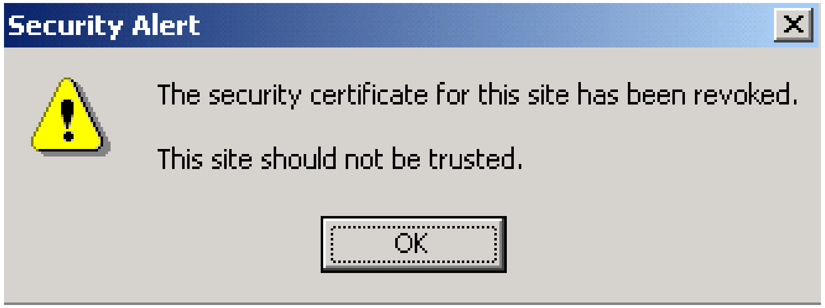
Accessing Web Sites That Issue Certificates

"Good" Status

- **Site certificate is valid and has not been revoked**
- **User is allowed to view the site with no warning or informational message**

"Bad" Status

- **Site certificate has been revoked**
- **Desktop Validator prevents user**

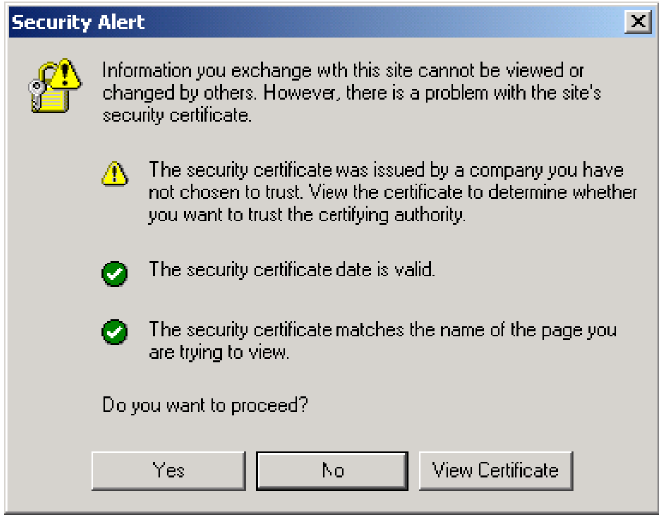


The security certificate for this site has been revoked.

This site should not be trusted.

"Unknown" Status

- **Validation information of the site certificate is not found**
- **User is given the option to proceed and view the site**



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

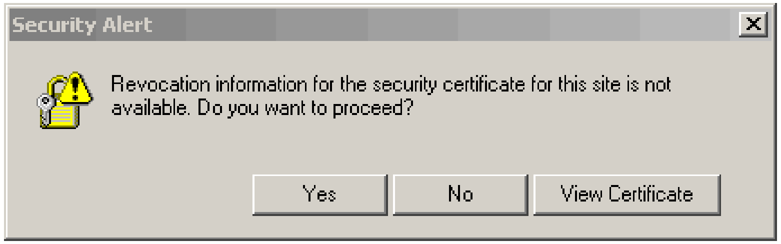
⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

✓ The security certificate matches the name of the page you are trying to view.

Do you want to proceed?

OR

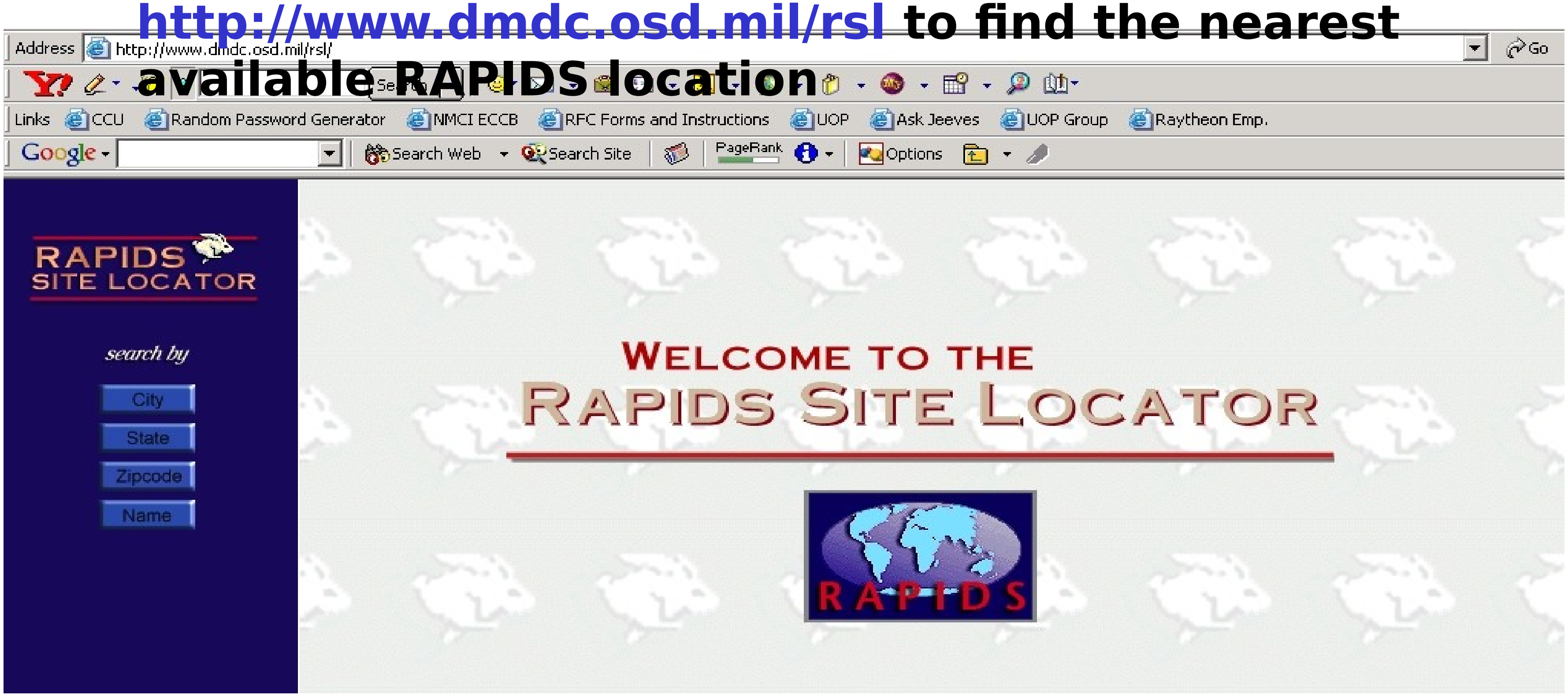


Revocation information for the security certificate for this site is not available. Do you want to proceed?

CAC Maintenance

Getting Your CAC Updated

- ✓ If your CAC is incomplete, incorrect, or locked, ***YOU MUST*** **visit a RAPIDS or CAC PIN Reset workstation**
- ✓ **Use RAPIDS Site Locator at http://www.dmdc.osd.mil/rsl to find the nearest available RAPIDS location**



Address http://www.dmdc.osd.mil/rsl/

WELCOME TO THE RAPIDS SITE LOCATOR

NMCI
NAVY MARINE CORPS INTRANET

Congratulations, you’re done!